Sub a30

WHAT IS CLAIMED IS:

1: A system for enabling asynchronous authentication of a non-preauthenticated client-User means in a Kerberos domain servicing multiple requesting non-preauthenticated clients while eliminating any delays due to multiple concurrent authentication requests, said system comprising:

(a) client-User means (10) for requesting authentication from a client-server means (13);

(b) client-server means (13) for communicating with a Kerberos server means (20) for developing a specific set of credentials for said single client requesting authentication;

(c) said Kerberos server means (20) for developing an asynchronous authentication response and a Ticket Granting Service to said client-server means (13).

2: The system of Claim 1 wherein said client-User means (10) includes:

(a1) multiple client-Users who may concurrently seek authorization to utilize said client-server.

3: The system of claim 1 wherein said Kerberos server means (20) includes:

(c1) means to return an authentication response to said client-Server means;

(c2) means to return a Ticket Granting Service signal to said client-server means.

4: The system of claim 1 wherein said client-server means includes:

(b1) communication means (MARC40, COMS42) for exchanging information between a requesting principal or client-User, a Master Control Program, a General Security Service Library (GSS38), and a Kerberos Support Library (KSL34);

(b2) said Master Control Program (60) for controlling said communication means, said General Security Service Library and said Kerberos Support Library (34);

(b3) said General Security Service Library (GSS38) providing multiple threads for handling multiple concurrent requests for authentication;

(b4) said Kerberos Support Library (34) for developing and storing specific authentication credentials for each validated client-User authentication request.

5: The system of claim 4 wherein said Kerberos Support Library (34) includes:

(b4a) means for accessing said Kerberos Server means (20) to acquire an authentication response and a Ticket Granting Service.

6: A secure message transmission system in a Kerberos environment which permits a client-user to operate in a network for authentication request transmittal and message response without suspending client service when a Kerberos Server has not yet responded to an earlier request for an authentication message code signal, said system comprising:

(a) client-terminal means (10) to indicate an original request for validation of an authentication message signal from a Kerberos Server (20);

(b) program means (MARC 40 and COMS 42), under control of a Master Control Program (MCP60), for transmitting requests for service to a Kerberos Support Library (34), a General Security Service Library (38) and Kerberos Server (20) for the return of an authentication response message to said client terminal means (10) from credential information placed in said General Security Service Library;

(c) means for enabling said Kerberos Support Library (34) to elicit authentication information and Ticket Granting Service from said Kerberos Server (20) for deposit as validating credential data in said General Security Service Library (38).

7: A method for asynchronous authentication of a non-preauthenticated originating terminal in a Kerberos domain, said authentication occurring without delay due to other concurrent requests for authentication by other terminals such as client-Users and principals, said method comprising the steps of:

(a) originating a request, to a client-server, for authentication by a non-preauthenticated terminal;

(b) processing said originating request and other originating requests concurrently;

(c) responding back asynchronously by said client-server to authenticate the validity of said original requesting terminal without any delays due to other concurrent requests for authentication.

8: The method of claim 7 wherein step (a) includes the step of:

(a1) originating concurrent multiple requests for authentication from multiple client-Users and principals.

9: The method of claim 7 wherein step (b) includes the steps of:

(b1) developing a set of identifying credentials for said originating terminal;

(b2) asynchronously validating said originating terminal for use of a Kerberos domain.

10: The method of claim 9 wherein step (b1) includes the steps of:

(b1a) requesting, via a communication means (MARC 40, COM942), under control of a Master Control Program (MCP60), a Kerberos Support Library (34), and a Kerberos Server (20) for credentials and a session key;

(b1b) creating a credential structure by said Kerberos Support Library (34) to identify said originating terminal and provide a Ticket Granting Service;

(b1c) generating, by a General Security Service Library (GSS 38), of a Name-Handle and GSS Credential Tag that identifies the originating terminal to said GSS (38) and to said Kerberos Support Library (34);

(b1d) generating a message, by said Kerberos Support Library (34), to inform said communication means (MARC 40, COMS42) that the Kerberos authentication cycle has been successfully completed.

11: The method of claim 9 wherein step (b1) includes the steps of:

(b1a) processing concurrent authentication requests via multi-threaded processing means to develop a specific credential for each originating terminal;

(b1b) conveying said first completed authentication request to said Kerberos Support Library (34) and said communication means (MARC 40, COMS42).

12: The method of claim 7 wherein step (c) includes the steps of:

(c1) utilizing said communication means (MARC 40, COMS42) to transmit an authentication signal from said Kerberos Support Library (34) to said originating terminal.

13: In a network wherein multiple client-terminals communicate with a client-server (13), having a Kerberos Support Library (34), and communicate with a communications means (MARC 40, COMS 42), a General Security Service Library (38) and said client-server for accessing response information from a Kerberos server (20), a method for enabling a requesting client-terminal to receive an authentication response message asynchronously from said Kerberos Server (20) comprising the steps of:

(a) initiating an authentication command request by a requesting client-terminal;

(b) utilizing a communication management system, under control at a Master Control Program (MCP60), using a communication means having a communication management program (COMS 42) and menu assisted resource control program (MARC 40) to communicate said command request to said Kerberos Server (20) via said Kerberos Support Library (34) and to receive a Kerberos response message for credential processing by said General Security Services Library (38) which is then conveyed by said communication means (40, 42) to said requesting client-terminal.

14: The method of claim 13 which includes the step of:

(c) Terminating the session between said client-terminal (10) and said Kerberos Support Library (34) once the authentication request response has been transmitted from said General Security Library (38), thus allowing said client-server (13) to process other authentication requests.

15: The method of claim 13 wherein step (b) includes the step of:

(b1) initiating an error message by said Kerberos Support Library (34) when a failure in authentication has been recognized;

(b2) requesting, via said error message, that said client-Terminal (b) should initiate a log-on.